

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
SOUTHEASTERN DIVISION**

IN RE DICAMBA HERBICIDES LITIGATION)	Master Case No.
)	1:18-md-02820-SNLJ
)	
)	MDL No. 2820
)	
)	<i>This Document Relates To All Cases</i>
)	

**STIPULATED PROTOCOL
FOR THE PRODUCTION OF DOCUMENTS AND ESI**

The parties in the above-captioned litigation (collectively, “the Parties”), by and through their respective counsel, have jointly stipulated to the terms of this Stipulated Protocol for the Production of Documents and Electronically Stored Information (the “ESI Protocol”).

I. SCOPE

A. Federal Rule of Civil Procedure 34 permits the Parties to specify the form or forms in which electronically stored information (“ESI”) is to be produced. Pursuant to Rule 34, this ESI Protocol shall govern the production of hard copy documents and other physical materials (“Documents”) and ESI by the Parties in the above-captioned consolidated MDL proceedings, including for all individual cases currently pending in MDL No. 2820 and cases that are later filed in, transferred to, or removed to this Court (the “Litigation”). The ESI Protocol shall also govern productions made by any third party who is subpoenaed in this Litigation, unless otherwise agreed to by the issuing party and the third party. Accordingly, this ESI Protocol shall be attached to any subpoena issued in this Litigation.

B. The ESI Protocol does not alter the Parties’ obligations to comply with the applicable Federal Rules of Civil Procedure and any applicable local rules regarding the production of Documents and ESI.

C. The Parties incorporate the provisions of the Order Establishing Protective Order (ECF Doc. 54).

D. Nothing in this ESI Protocol establishes any agreement regarding the subject matter or scope of discovery in this Litigation, or the relevance, authenticity, or admissibility of any Documents or ESI.

E. Nothing in this ESI Protocol shall be interpreted to require production of Documents or ESI protected from disclosure by the attorney-client privilege, work product doctrine, common interest privilege, or any other applicable protection or privilege. Nor shall this ESI Protocol be interpreted to require production of Documents or ESI prohibited from disclosure under any similar law, regulation, rule, or court order. The Parties do not waive any objections to the production, discoverability, or confidentiality of Documents, ESI, or any other discovery materials, including but not limited to: objections regarding the proportionality of the discovery request or the burden, overbreadth, or relevance of Documents, ESI, or any other discovery materials.

F. Any Party that produced documents prior to the February 1, 2018 Transfer Order of the Judicial Panel on Multidistrict Litigation shall produce those documents in this Litigation as they were produced in the prior action or proceeding. These documents are not required to comply with this ESI Protocol nor is the party producing such documents (the “Producing Party”) required to provide any additional metadata overlay for these documents. Nothing in this Order obligates a party to re-produce processed or produced documents, unless those same documents or materials are also retrieved as a matter of course in connection with processing ongoing ESI searches.

G. Any practice or procedure set forth herein may be varied by written agreement of the Parties.

II. IDENTIFICATION OF CUSTODIANS AND SEARCH METHODOLOGY

The procedure, scope, and limitations governing identification of custodians; identification and application of ESI search terms; and the timing and deadlines for conducting custodian-based ESI production will be set forth in a separate, forthcoming Stipulated ESI Custodian and Search Terms Protocol or order of court.

III. PRODUCTION FORMAT

A. Paper Documents: Paper records will be scanned or otherwise converted into electronic form from paper Documents in the following format:

1. TIFFs. All Documents shall be scanned to single page Group 4, TIFF format, at least 300 dpi and 8 ½ x 11 inch page size, except for Documents requiring higher resolution or different page size. Documents with color in native format (e.g., color photographs or graphical representations) should be imaged to single page, JPEG format, to retain color. Each image file should have a unique file name which shall be the Bates number of the page.

2. In scanning paper Documents, images of Documents will be organized according to the manner in which they were maintained in the ordinary course of business, including, where available, copies of file folders, envelopes, or labels or other identifying marks on the containers in which the Documents were maintained, or organized and labeled to correspond to the categories in the document requests. In addition, where a paper document has “post-it” notes or any other affixed labels, the information on the label and/or note shall be scanned and produced to the extent practicable. Distinct Documents should not be merged into a single record, and single Documents should not be split into multiple records (i.e., paper Documents

should be logically unitized). The Parties will make their best efforts to have their vendors unitize Documents correctly and will commit to address situations where there are improperly unitized documents.

3. Coding Fields. The following coding fields should be provided, if applicable:

Field Name	Field Description
BegBates	Beginning Bates# (including Prefix)
EndBates	Ending Bates# (including Prefix)
BegAttach	Beginning Bates number of the first document in an attachment range (only in emails with attachments)
EndAttach	Ending Bates number of the last document in attachment range (only in emails with attachments)
PgCount	Number of pages in the item
Custodian	Name of Custodian(s) of document (Last Name, First Name format) as available
Confidentiality Designation	The designated level of confidentiality pursuant to the Protective Order.
Redacted	User-generated field that will indicate redactions using "Y" for yes and "N" or Blank for no redaction.

B. Electronically Stored Information: The Parties will produce ESI in TIFF format according to the following specifications:

1. All TIFF formatted documents will be single page, Group 4 TIFF at 300 X 300 dpi resolution and 8½ X 11 inch page size, except for documents requiring different resolution or page size. The requesting party retains the right to request a TIFF image in a higher resolution or larger page size if necessary to render the image legible or reasonably usable.

2. To the extent practicable, each individual document based on an electronic file shall be accompanied by a corresponding text file with text that is extracted from the electronic file. The exception to this will be redacted documents, as discussed below.

3. An image load file, in standard Opticon format (OPT), standard IPro format (LFP), or standard Summation format (DII), showing the Bates number of each page and the appropriate unitization of the documents, will accompany all document images.

4. Each imaged version of an electronic document will be created directly from the original electronic document. Word processing files, including Microsoft Word files, will be produced with tracked changes and comments showing and searchable in the extracted text. Documents that contain languages other than English, in whole or in part, shall be produced in the original language(s).

5. The following metadata fields associated with each electronic document will be produced.

Field Name	Field Description	Required for Email	Required for Non-E-mail ESI
Custodian	Name of Custodian(s) of email(s) or file(s) produced (Last Name, First Name format) as available	x	x
Duplicate Custodian (if globally deduplicated)	Name of duplicate Custodian(s) of email(s) or file(s) produced	x	x
BegBates	Beginning Bates# (including Prefix)	x	x
EndBates	Ending Bates# (including Prefix)	x	x
BegAttach	Beginning Bates number of the first document in an attachment range (only in emails with attachments)	x	x
EndAttach	Ending Bates number of the last document in attachment range (only in emails with attachments)		
From	From field extracted from an email message	x	
Author	Author field extracted from the metadata of a non-email document		x
To	To or Recipient extracted from an	x	

Field Name	Field Description	Required for Email	Required for Non-E-mail ESI
	email message		
Cc	Carbon Copy (“Cc”) field extracted from an email message	x	
Bcc	Blind Carbon Copy (“Bcc”) field extracted from an email message	x	
EmailSubject	Subject line extracted from an email message	x	
Filename	File name — Original name of file as appeared in original location		x
Title	Title field extracted from the metadata of a non-email document		x
DateSent	Sent date of an email message (mm/dd/yyyy format) (a given email will have either a DateSent or Date Recvd, but not both)	x	
DateRcvd	Received date of an email message (mm/dd/yyyy format) (a given email will have either a DateSent or Date Recvd, but not both)	x	
DateCreated	Date that a non-email file was created (mm/dd/yyyy format)		x
Date Last modified	The application recorded time on which the document was last modified		x
TimeSent	Time e-mail was sent (hh:mm:ss format) (a given email will have either a TimeSent or Time Recvd, but not both)	x	
TimeRcvd	Time e-mail was received (hh:mm:ss format) (a given email will have either a TimeSent or Time Recvd, but not both)	x	
File Path	File path storage location of the document or email if the source application allows for the creation of folders	x	x
Native Link	Relative path to any files produced in	x	x

Field Name	Field Description	Required for Email	Required for Non-E-mail ESI
	native format		
Text Link (if text is exchanged)	Relative path to any OCR/extracted text files in the production set	x	x
Confidentiality Designation	The designated level of confidentiality pursuant to the Protective Order.	x	x
Hash Value	MD5 or SHA-1 hash value used to deduplicate the data	x	X
Redacted	User-generated field that will indicate redactions using “Y” for yes and “N” or Blank for no redaction.		

6. The Parties will produce the following ESI types in native file format: (a) spreadsheets; (b) audio/video files; (c) PowerPoint presentations; and (d) any files that cannot be imaged.

7. Any document produced in native format, will be produced according to the following specifications:

- a. A unique bates number and confidentiality designation (if applicable) shall be used as the file name and the original file name and file extension shall be preserved in the corresponding load file.
- b. The native format documents shall be accompanied by reference information that sets forth for each document, sufficient information to allow the Parties to track and authenticate the native format documents produced, including: (i) the name of the custodian from whose files the electronic file is produced; (ii) an appropriately calculated “MD-5 Hash Value”; and (iii) the original name of the file.

- c. Any file produced in native format need not be imaged. Instead, a single page placeholder image shall be provided that indicates the file was produced in native format and contains the bates number of the corresponding file and any confidentiality designation.

8. OLE embedded objects (embedded MS Office files, etc.) shall be extracted as separate files and treated as attachments to the parent document. Images embedded in emails shall not be produced as attachments unless they are responsive to a discovery request served upon the Producing Party.

9. Absent good cause shown, a party is not required to preserve, search, collect, review, or produce the following categories of electronic files:

- a. Any electronic file which matches the Reference Data Set published by the National Institute of Standards and Technology's National Software Reference Library.
- b. System or executable files (.exe, .dll, etc.).
- c. Structural files not material to individual file contents that do not contain substantive content (.css, .xsl, .xml, .dtd, etc.).
- d. Backup data files that are maintained in the normal course of business for purposes of disaster recovery, including backup tapes, disks, SAN, and other forms of media, and that are substantially duplicative of data that are more accessible elsewhere. Absent a party's specific written notice for good cause, no party shall be required to modify or suspend procedures, including rotation of backup media, used in the usual course of business to back up data and systems for data recovery purposes.

- e. Deleted, slack, fragmented, or unallocated data.
- f. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.
- g. On-line access data such as temporary internet files, history files, cache files, and cookies.
- h. Data in metadata fields frequently updated automatically, such as last-opened or last-printed dates.
- i. Instant messages, text messages, and voicemail not retained in the usual course of business or pursuant to a litigation hold for the Litigation.
- j. Data remaining from systems no longer in use that are unreadable on the systems in use.

9. No party shall be required to modify or suspend procedures, including rotation of backup media, used in the normal course of business to back up data and systems for disaster recovery purposes.

C. Redacted Files

1. Extracted text will not be provided for ESI that has been redacted—*e.g.*, for privilege or trade secrets—because the extracted text would reveal the redacted information. Instead, these files should be run through an OCR process to capture the visible text only and the results exchanged in lieu of the original extracted text. The portion of the redacted text shall be clearly identified on the face of the TIFF image, either by masking the redacted content with electronic highlighting in black or through the use of redaction boxes.

D. Data Load Files/Cross-Reference Files

Fielded data should be exchanged via a document-level-database load file in one of two delimited formats. Either standard Concordance (DAT) or comma delimited (CSV). All image data should be delivered with a corresponding image load file in one of three formats; standard IPro (LFP), Opticon (OPT) or Summation (DII). The total number of images files referenced in the image load file should match the total number of images in the production delivery.

E. Deduping Documents and Most Inclusive Email Productions

“Duplicate ESI” are exact duplicates based on the files’ MD5 or SHA-1 Hash Value. The Parties may dedupe documents including within each custodian or globally (i.e., across all Custodians). This will result in the Producing Party needing to produce only a single copy of responsive Duplicate ESI, provided that all other Custodians of the Duplicate ESI are listed in the “Custodians” or “Duplicate Custodian” field. The Producing Party agrees that the presence of a custodian’s name listed in the “Custodian” or “Duplicate Custodian” field is evidence that a duplicate of the document was located in that custodian’s file. The Parties shall de-duplicate stand-alone documents against stand-alone documents and shall de-duplicate top-level email documents against top-level email documents. De-duplication shall not break apart families. No document that is the parent or an attachment of a produced document may be withheld as a duplicate. In order to reduce the volume of entirely duplicative content within email threads, the Parties may but are not required to use email thread suppression. A Producing Party will agree to produce metadata for suppressed emails upon reasonable request.

F. Databases.

A Party possessing databases that contain relevant information shall produce the information in the agreed upon format for ESI, in Excel, or Access, except where the Requesting

Party can show particularized need for another format. The Parties agree to meet and confer in good faith regarding discovery from relevant and proportional applications and databases.

G. Encrypted Data/Password Protected Files

Certain files may contain encrypted data or be password protected. When the key or password can be obtained through reasonable efforts, a Producing Party should apply the appropriate key or password to the file and produce the file unencrypted. If the party cannot obtain the key or password through reasonable efforts, the Producing Party should provide the file's metadata in accordance with Section III.B in the production load file and a slip-sheet should be included in the image set, stating the file is an exception.

H. Residual, Fragmented, Damaged, or Temporary Data

Parties reserve the right to not produce the following ESI files provided the Party identifies the file metadata that meet any search term criteria: data stored in a computer's RAM, any data on unreadable or damaged disc sectors, readable data stored in proprietary format determined to be corrupted by the software capable of rendering the format, and data that would require forensic reconstruction.

I. Parent-Child Relationships for ESI Documents

Parent-child relationships (the association between an attachment and its parent document) shall be preserved to the extent possible. Attachments are to be produced contemporaneously and sequentially immediately after the parent document. Non-responsive attachments may be excluded from production. Non-responsive attachments excluded from production shall be produced as a Bates-numbered placeholder. The Parties will confer in good faith regarding any dispute over responsiveness of withheld attachments. Where the attachment (child document) is produced, the parent document associated with the attachment shall be

produced regardless of whether it is responsive or itself contains an ESI search term. The parent document associated with the responsive attachment will not be produced if it is protected by attorney-client privilege, the attorney work product doctrine, and/or any other applicable privilege; the privilege log entry for the withheld parent document will indicate the bates number of the produced attachment. The Producing Party may redact Confidential or Highly Confidential Discovery Material contained within the parent document in accordance with the Order Establishing Protective Order (ECF Doc. 54) if the Confidential or Highly Confidential Discovery Material is unrelated to the responsive attachment.

IV. PRODUCTION OF DISCOVERY MATERIALS CONTAINING POTENTIALLY PRIVILEGED OR PROTECTED INFORMATION

A. In accordance with Paragraph 14 of the Order Establishing Protective Order (ECF No. 54) regarding protections from waiver of the disclosure of attorney-privileged or work-product protected information under Federal Rule of Evidence 502(d), the Parties shall follow the procedure set forth in Federal Rule of Civil Procedure 26(b)(5)(B) regarding the claw back of potentially privileged or protected discovery materials. To that end, a Producing Party shall notify any Party that received the information of the claim and the basis for it. After being notified, a Party must, consistent with Paragraph IV.B., promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the Information until the claim is resolved; must take reasonable steps to retrieve the Information if the Party disclosed it before being notified; and promptly present the Information to the Court under seal for a determination of the claim. The Producing Party must preserve the Information until the claim is resolved.

B. Prior to seeking resolution with the Court, the Parties shall first meet and confer within fourteen (14) days of notification of the production of such Information to resolve any

disagreement over whether the Information is protected by attorney-client privilege, attorney work product doctrine, and/or any other applicable privilege. Within seven (7) days of conclusion of the meet and confer process, the Receiving Party must file a motion with the Court seeking resolution of any remaining disagreement as to whether the Information is protected by attorney-client privilege, attorney work product doctrine, and/or any other applicable privilege. The Receiving Party may not challenge the privilege or immunity claim by arguing that the disclosure of the Information itself is a waiver of any applicable privilege.

C. Any analyses, memoranda or notes which were internally generated based upon such produced Information shall immediately be placed in sealed envelopes, and shall be destroyed in the event that (a) the Receiving Party does not contest that the Information is privileged, or (b) the Court rules that the Information is privileged. Such analyses, memoranda or notes may only be removed from the sealed envelopes and returned to its intended purpose in the event that (a) the Producing Party agrees in writing that the Information is not privileged, or (b) the Court rules that the Information is not privileged.

V. PRIVILEGE LOGGING

A. The Producing Parties will produce privilege logs in Excel format or a similar electronic format that allows text searching and organization of data, which will include at least the following fields: Bates #; Custodian; Date; To; From; CC; BCC; attorney-client privilege, attorney work product doctrine, and/or any other applicable privilege asserted; and basis for such assertion in compliance with the Federal Rules of Civil Procedure, applicable case law, and the Local Rules of this Court. The parties agree to meet and confer in good faith regarding any disputes as to privilege logs.

B. The following documents presumptively need not be included on a privilege log:

- i. Written or oral communications between a Party and its counsel after commencement of the first-filed lawsuit that it was named as Party in and is part of this Litigation (“First Lawsuit”) as it related to the conduct of that First Lawsuit and/or other anticipated litigation; or
- ii. Work product created by outside counsel, or by an agent of outside counsel (other than a Party) after commencement of the First Lawsuit that is purely related to the prosecution of that First Lawsuit and/or other anticipated litigation. The parties also shall not be required to include on a privilege log written or oral communication with experts retained after commencement of the First Lawsuit and/or other anticipated litigation. Expert disclosures shall be governed by the case management order.

C. An email thread for which a Party claims a privilege may be logged in a single entry. With respect to e-mail threads for which a Party claims a privilege, only the most inclusive e-mail shall be logged. However, the log will list any outside parties on the withheld e-mail thread that are not reflected in the metadata and the log will note their relationship to the Party. If an email thread contains both privileged and non-privileged emails, the responsive non-duplicative, non-privileged emails should be produced and any privileged emails withheld and logged.

So ordered this 23rd day of July 2018.



STEPHEN N. LIMBAUGH, JR.
UNITED STATES DISTRICT JUDGE